SPYWOLF

Security Audit Report

Completed on
July 12, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **BLACKSHEEP** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

" *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal* "

– SPYWOLF Team –

TABLE OF CONTENTS

BLACKSHEEP

Blacksheep

PROJECT DESCRIPTION

According to their whitepaper:

$SHEEPLE is a BINANCE SMART CHAIN TOKEN deployed on JUNE, 2022

The max supply is 1 Quadrillion and one of its key functionalities is its decentralised finance protocol.

Future development of the project will be as follows:

- NFTs
- Staking
- P2E game

Release Date: Launched on July 06, 2022

Category: NFT/P2E

01

CONTRACT INFO

Token Name
BlackSheep

Symbol
SHEEPLE

Contract Address
0x8eE162bcF27F1Da9799C36ff013a2Ace29e62CBD

Network
Binance Smart Chain

Language
Solidity

Deployment Date
July 04, 2022

Verified?
Yes

Total Supply
1,000,000,000,000,000

Status
Launched

TAXES

Buy Tax
9%

Sell Tax
9%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

02

CURRENT STATS

(As of July 12, 2022)

Liquidity

PancakeSwap:
157 WBNB

Burn

36.1% of total supply

Status:
Launched!

MaxTxAmount
NoLimit

DEX:
PancakeSwap

LP Address(es)

Pancakeswap:
0x19247c0D24103b5e14D7A489B0c59d6a08F4442C

97.59% locked in PinkLock - unlocks at 2023.07.05
https://www.pinksale.finance/pinklock/record/1014257?chain=BSC

Locked wallet(s)

0x407993575c91ce7643a4d4ccacc9a98c36ee1bbe

25% locked for vesting in PinkLock at 7 days cycle (20% of which,
already released) - TGE date 2022.07.05 17:00
https://www.pinksale.finance/pinklock/record/1014020?chain=BSC

03

SPYWOLF.CO

TOKEN TRANSFERS STATS

Transfer Count	3400
Uniq Senders	658
Uniq Receivers	1504
Total Amount	5472485012069606 SHEEPLE
Median Transfer Amount	112863969206.03383 SHEEPLE
Average Transfer Amount	1609554415314.5898 SHEEPLE
First transfer date	2022-07-04
Last transfer date	2022-07-12
Days token transferred	9

SMART CONTRACT STATS

Calls Count	8517
External calls	912
Internal calls	7605
Transactions count	3374
Uniq Callers	789
Days contract called	8
Last transaction time	2022-07-12 05:57:28 UTC
Created	2022-07-05 09:34:37 UTC
Create TX	0x0d7f83f99d6e74f3014af3784a2962303cdee3667dc6b47c0c0edfb08f1ae7c6
Creator	0xa90d5c13033d0b1b503ac102dc900940def3fcab

04

FEATURED WALLETS

Owner address	0xa90d5c13033d0b1b503ac102dc900940def3fcab
Marketing wallet	Same as owner
LP address	**Pancakeswap:** 0x19247c0D24103b5e14D7A489B0c59d6a08F4442C 97.59% locked in PinkLock - unlocks at 2023.07.05 https://www.pinksale.finance/pinklock/record/1014257?chain=BSC

TOP 3 UNLOCKED WALLETS

1

0.43% 0x569b6a13d0c1a6d31b1a397cc5fb20e690a0069b

2

0x6eae6ab0745c9261f0d0bb4663e008cb0cd3cf9d **0.35%**

3

0.34% 0x1a0558a4125c3ee091da206c258a6c76b9464193
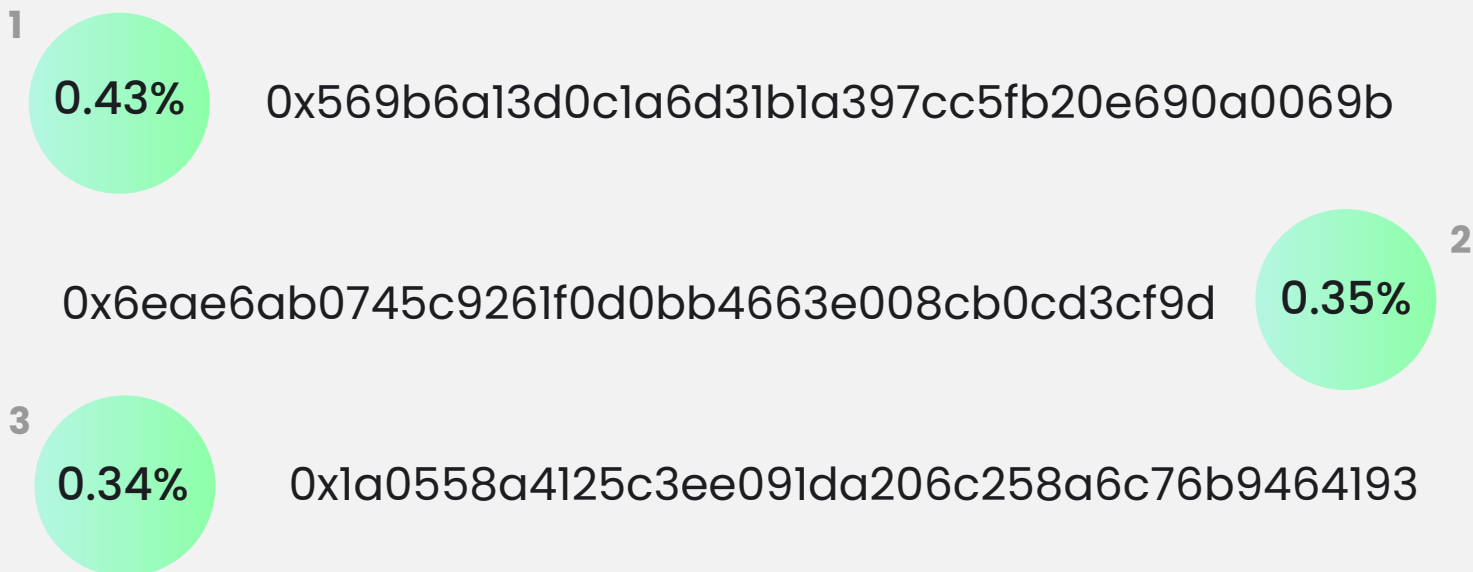
VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

06

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

07

FOUND THREATS

⚠️ High Risk

Owner can change max holdings limit per wallet.
Owner can set max transaction limit, based on % of user's holdings.
If the liquidity pair is not excluded from limitations, all transfers will be subject to max transaction and max wallet limit, including ones from/to LP.
This will lead to inability to sell when the LP holdings are above max wallet limits.
If the limits for max transaction are set too low, fees associated with the transfer can be higher than transferred tokens value.

```solidity
function SetLimit(uint LimitV2) public onlyTeam{
    LimitV=LimitV2;
    emit OnSetLimit(LimitV2);
}

function SetSell(uint LimitSell2) public onlyTeam{
    LimitSell=LimitSell2;
    emit OnSetSell(LimitSell2);
}

function _taxedTransfer(address sender, address recipient, uint amount) private{
    uint senderBalance = _balances[sender];
    uint recipientBalance = _balances[recipient];
    require(senderBalance >= amount, "Transfer exceeds balance");
    require(senderBalance/LimitSell >= amount, "Transfer exceeds authorise sell");
    require((recipientBalance + amount ) <= InitialSupply/LimitV,
    "Wallet contain more than certain % Total Supply");
    ..............
}
```

08-A

FOUND THREATS

⚠️ Medium Risk

Owner can set buy taxes up to 20%, sell taxes up to 20% and transfer taxes up to 20%.

```solidity
uint constant TAX_DENOMINATOR=1000;
uint constant MAXTAXDENOMINATOR=10;

function SetTaxes(uint buy, uint sell, uint transfer_,
 uint burn, uint marketing,uint liquidity) public onlyTeam{
    uint maxTax=2*(TAX_DENOMINATOR/MAXTAXDENOMINATOR);
    require(buy<=maxTax&&sell<=maxTax&&transfer_<=maxTax,"Tax exceeds maxTax");
    require(burn+marketing+liquidity==TAX_DENOMINATOR,"Taxes don't add up to denominator");

    buyTax=buy;
    sellTax=sell;
    transferTax=transfer_;
    marketingTax=marketing;
    liquidityTax=liquidity;
    burnTax=burn;
    emit OnSetTaxes(buy, sell, transfer_, burn, marketing,liquidity);
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

08-B

FOUND THREATS

⚠️ Medium Risk

Owner can exclude address from fees and transaction limits.

```
function ExcludeAccountFromFees(address account, bool exclude) public onlyTeam{
    require(account!=address(this),"can't Include the contract");
    excludedFromFees[account]=exclude;
    emit ExcludeAccount(account,exclude);
}

function ExcludedFromLimit(address account, bool exclude) public onlyTeam{
    require(account!=address(this),"can't Include the contract");
    excludedFromLimit[account]=exclude;
    emit ExcludeAccountLimit(account,exclude);
}
```

08-c

ℹ️ Informational

Accumulated LP tokens from fees in the contract can be locked and withdrawn each 7 days.

```solidity
uint _liquidityUnlockTime;
bool public LPReleaseLimitedTo20Percent;
//Sets Liquidity Release to 20% at a time and prolongs liquidity Lock for a Week after Release.
//That way autoLiquidity can be slowly released
function limitLiquidityReleaseTo20Percent() public onlyTeam{
    LPReleaseLimitedTo20Percent=true;
}


//Locks Liquidity for seconds. can only be prolonged
function LockLiquidityForSeconds(uint secondsUntilUnlock) public onlyTeam{
    _prolongLiquidityLock(secondsUntilUnlock+block.timestamp);
}


event OnProlongLPLock(uint UnlockTimestamp);
function _prolongLiquidityLock(uint newUnlockTime) private{
    // require new unlock time to be longer than old one
    require(newUnlockTime>_liquidityUnlockTime);
    _liquidityUnlockTime=newUnlockTime;
    emit OnProlongLPLock(_liquidityUnlockTime);
}


event OnReleaseLP();
//Release Liquidity Tokens once unlock time is over
function LiquidityRelease() public onlyTeam {
    //Only callable if liquidity Unlock time is over
    require(block.timestamp >= _liquidityUnlockTime, "Not yet unlocked");

    IBEP20 liquidityToken = IBEP20(_pancakePairAddress);
    uint amount = liquidityToken.balanceOf(address(this));
    if(LPReleaseLimitedTo20Percent)
    {
        _liquidityUnlockTime=block.timestamp+DefaultLiquidityLockTime;
        //regular liquidity release, only releases 50% at a time and locks liquidity for another week
        amount=amount*5/10;
    }
    liquidityToken.transfer(msg.sender, amount);
    emit OnReleaseLP();
}
```

08-D

RECOMMENDATIONS FOR

GOOD
PRACTICES

1 Consider fundamental tradeoffs

2 Be attentive to blockchain properties

3 Ensure careful rollouts

4 Keep contracts simple

5 Stay up to date and track development
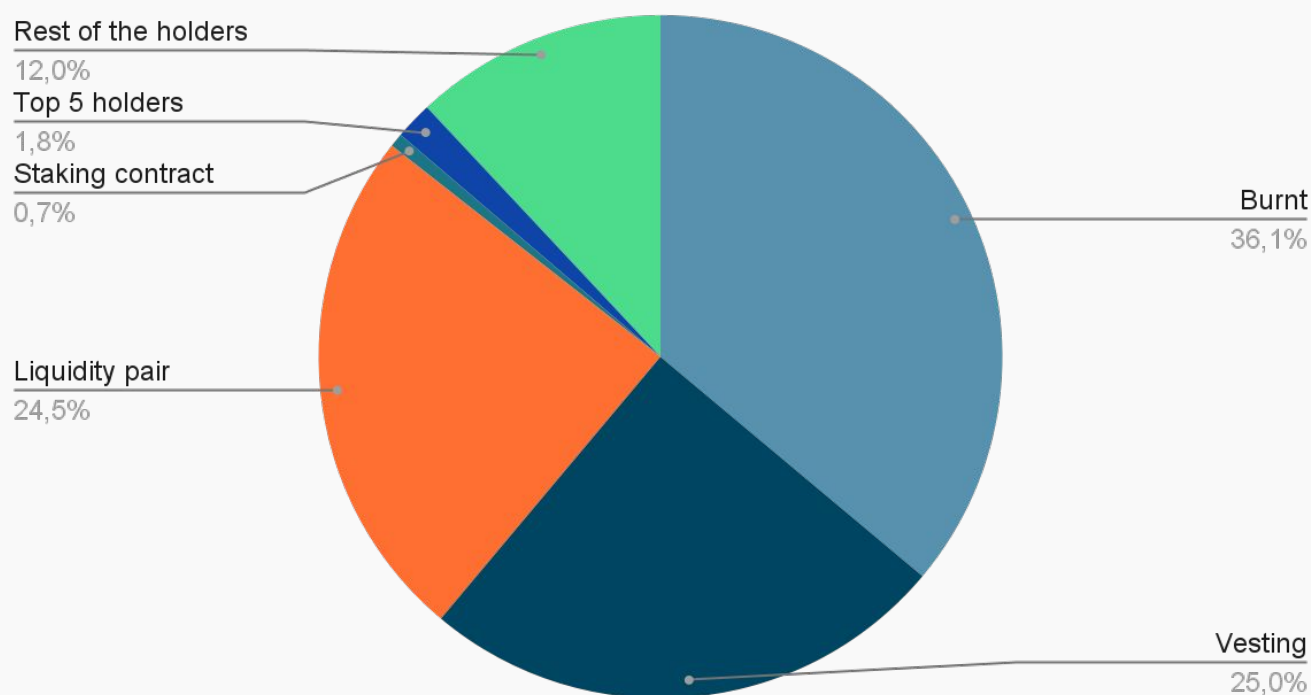
BLACKSHEEP

GOOD PRACTICES FOUND

✔ The owner cannot mint new tokens after deployment

09

Current state according to BSCscan:

- 36.1% - Burnt
- 25% - Vesting
- 24.5% - Liquidity pair
- 0.65% - Staking contract
- 1.78% - Top 5 holders
- 11.97% - Rest of the holders

Tokens distribution

Rest of the holders
12,0%

Top 5 holders
1,8%

Staking contract
0,7%

Liquidity pair
24,5%

Burnt
36,1%

Vesting
25,0%

*For more information about vesting periods and amounts released visit the link:
https://www.pinksale.finance/pinklock/record/1014020?chain=BSC

THE TEAM

⚠️ **The team is annonymous**

KYC INFORMATION

⚠️ **No KYC**

We recommend the team to get a KYC in order to ensure trust and transparency within the community.

KYC
ERTIFICAT

ISSUED ON
MAY 31, 2022

11

Website URL
https://www.black-sheep.xyz/

Domain Registry
https://publicdomainregistry.com

Domain Expiration
Expires on 2023-05-25

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page, appropriate color scheme and graphics.

Content
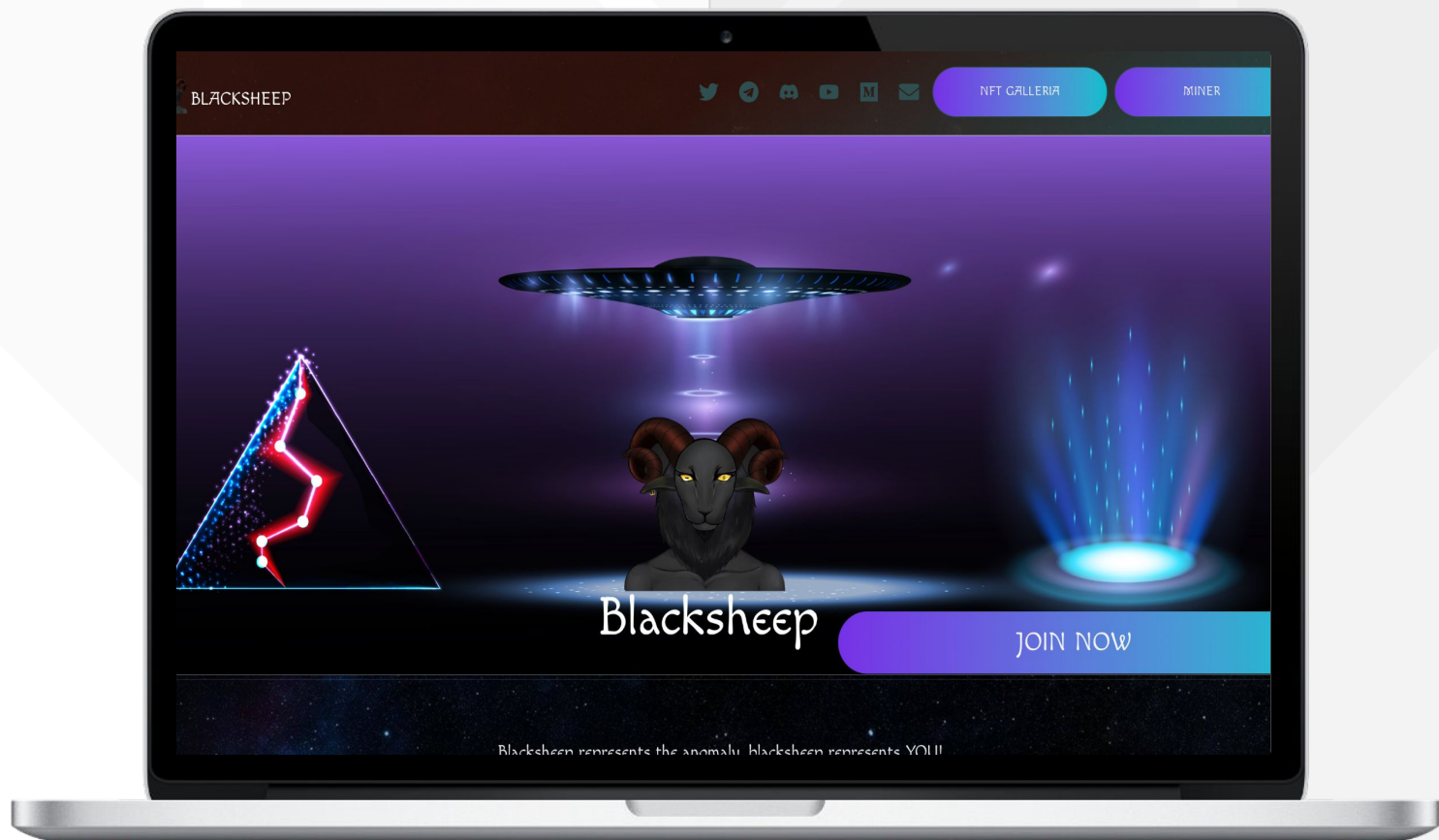The information helps new investors understand what the product does right away.

Whitepaper
Well written, explanatory.

Roadmap
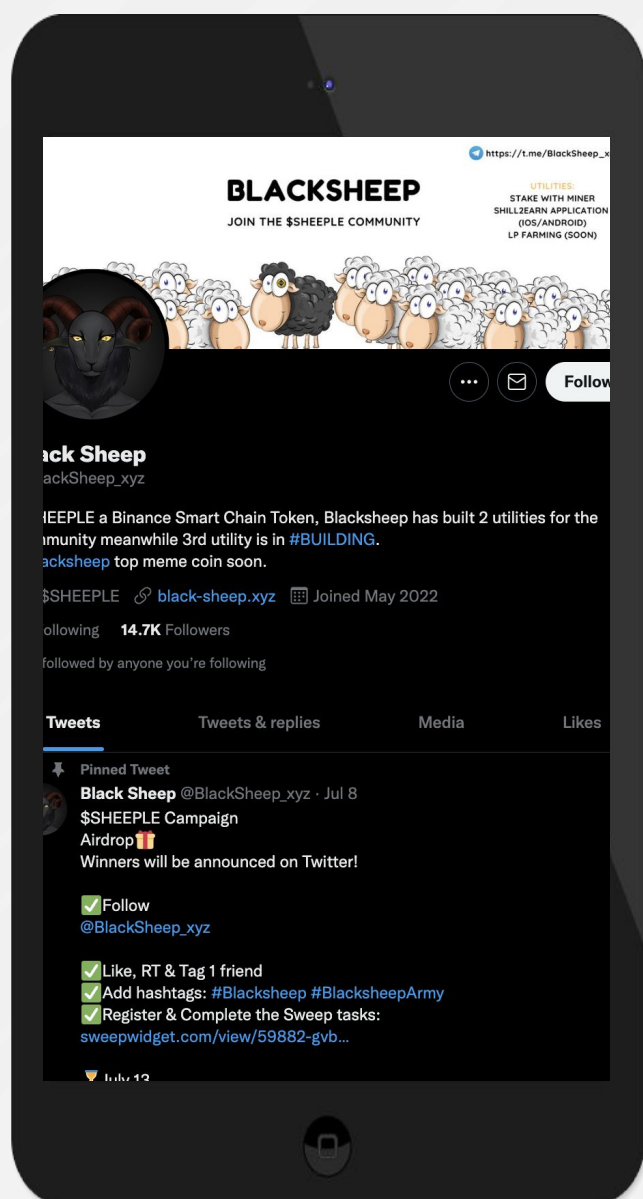Yes, goals set without timeframes.

Mobile-friendly?
Yes

black-sheep.xyz
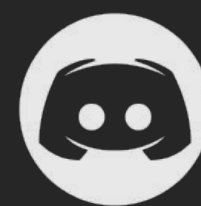
SOCIAL MEDIA
& ONLINE PRESENCE

ANALYSIS
Project's social media accounts are active!

Twitter

https://twitter.com/BlackSheep_xyz

- 14 500 followers
- Active
- Daily posts

Discord

https://discord.com/invite/tZD8kzFw7n

- 1 166 members
- Few active members

Telegram

https://t.me/BlackSheep_XYZ

- 14 009 members
- Active members
- Active mods

Medium

https://medium.com/@blacksheep.eth

- 2 articles

SPYWOLF
CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✔ **OVER 150 SUCCESSFUL CLIENTS**
- ✔ **MORE THAN 500 SCAMS EXPOSED**
- ✔ **MILLIONS SAVED IN POTENTIAL FRAUD**
- ✔ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- ✔ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to contact@spywolf.co or t.me/joe_SpyWolf

FIND US ONLINE

🌐 **SPYWOLF.CO**

🌐 **SPYWOLF.NETWORK**

✈ **@SPYWOLFNETWORK**

✈ **@SPYWOLFOFFICIAL**

🐦 **@SPYWOLFNETWORK**

@SPYWOLFNETWORK

14

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.